

NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



THESIS

THE WARFIGHTERS' FUTURE LINK TO INFORMATION

by

Christopher B. Henderson

June 1996

Co-Advisors:

Dan C. Boger
Rex A. Buddenberg

Approved for public release; distribution is unlimited.

19960910 006

REPORT DOCUMENTATION PAGE			Form approved OMB No. 0704-188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information including suggestions for reducing this burden, to Washington Headquarters services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE June 1996	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE THE WARFIGHTERS' FUTURE LINK TO INFORMATION (U)			5. FUNDING NUMBERS	
6. AUTHOR(S) Henderson, Christopher B..				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) <p>The purpose of this thesis is to introduce the concept of having a jointly integrated networkin schema to better enhance battlefield communications and the dissemination of information using a smart push/pull concept from the highest commander down to the individual soilder. The concept of having a robust and dynamic network couls provide the United States Armed Forces a better way of integrating the individual soilder's performance into higher level units. Current systems in the armed forces inventory are not truly interoperable, and not everyone has the capability to receive the information that these systems carry. A networked battlefield would allow everyone on the network to receive data carried by all systems.</p> <p>With smart integration and design using commercially tested standards, the network can be built for all battlefield components. Each component would bring its equipment into the battlefield and become part of the network. Their systems would be able to plug and play with all other systems in the battlefield. The liberal use of COTS and GOTS networking equipment will reduce the cost of the network and would ensure compatibility among the battlefield components. Using OSI layers in the design of the system would ensure compatibility. DOD would need to make a concerted effort by having all of the services agree to make the battlefield network a top priority.</p>				
14. SUBJECT TERMS COTS, commercial-of-the-shelf, GOTS, government-off-the-shelf, net-centric, OSI			15. NUMBER OF PAGES 70	
			16. PRICE CODE	
17. SECURITY CLASSIFI- CATION OF REPORT Unclassified	18. SECURITY CLASSIFI- CATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFI- CATION OF THIS ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std Z39-18**DTIC QUALITY INSPECTED 3**

THE UNIVERSITY OF CHICAGO

Approved for public release; distribution is unlimited.

THE WARFIGHTERS' FUTURE LINK TO INFORMATION

Christopher B. Henderson
Lieutenant, United States Navy
B.S., Auburn University, 1988

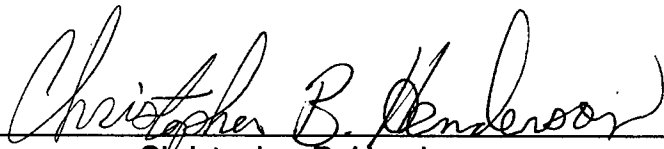
Submitted in partial fulfillment of
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL AND COMMUNICATIONS SYSTEMS)**


from the

**NAVAL POSTGRADUATE SCHOOL
June 1996**

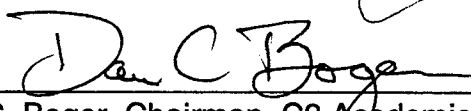
Author:


Christopher B. Henderson

Approved by:


Dan C. Boger, Co-Advisor


Rex Buddenberg, Co-Advisor


Dan C. Boger, Chairman, C3 Academic Group

ABSTRACT

The purpose of this thesis is to introduce the concept of having a jointly integrated networking schema to better enhance battlefield communications and the dissemination of information using a smart push/pull concept from the highest commander down to the individual soldier. The concept of having a robust and dynamic network could provide the United States Armed Forces a better way of integrating the individual soldier's performance into higher level units. Current systems in the armed forces inventory are not truly interoperable, and not everyone has the capability to receive the information that these systems carry. A networked battlefield would allow everyone on the network to receive data carried by all systems.

With smart integration and design using commercially tested standards, the network can be built for all battlefield components. Each component would bring its equipment into the battlefield and become part of the network. Their systems would be able to plug and play with all other systems in the battlefield. The liberal use of COTS and GOTS networking equipment will reduce the cost of the network and would ensure compatibility among the battlefield components. Using OSI layers in the design of the system would ensure compatibility. DOD would need to make a concerted effort by having all of the services agree to make the battlefield network a top priority.

Table of Contents

I. INTRODUCTION	1
A. PURPOSE OF THESIS	1
B. BACKGROUND	2
C. SCOPE	4
II. CURRENT TACTICAL SYSTEMS	7
A. OVERVIEW	7
B. LINK-11	7
C. LINK-4A	10
D. LINK-16	12
E. GLOBAL BROADCAST SYSTEM (GBS)	15
F. VOICE COMMUNICATIONS	16
G. SUMMARY	17
III. OBJECTIVES AND DOCTRINE	19
A. C4 SYSTEMS OBJECTIVES	19
B. BASIC DOCTRINE FOR C4 SYSTEMS	21
C. NET-CENTRIC CONCEPT	23
D. BENEFITS OF A BATTLEFIELD NETWORK	26
IV. THE NETWORK VISION	29
A. THE BIG PICTURE	29
B. DESIGN ISSUES	32
V. CLOSE AIR SUPPORT SCENARIO	41
A. BACKGROUND	41
B. PREFLIGHT	41
C. FLIGHT MISSION	41
D. POST MISSION	45
E. SUMMARY	45
VI. CONCLUSIONS AND RECOMMENDATIONS	47
A. CONSLUSIONS	47
B. RECOMMENDATIONS	48
LIST OF REFERENCES	51
INITIAL DISTRIBUTION LIST	53

List of Figures

Figure 1	Link-11 Star Topology	7
Figure 2	Link-11 Polling	9
Figure 3	Link-11 Components	9
Figure 4	Link-4A Net.....	10
Figure 5	Link-4A Equipment Configuration.....	11
Figure 6	Link-16 System	13
Figure 7	Link-16 Stacked Net.....	13
Figure 8	Network Subsection	25
Figure 9	The Evolution of C4I for the Warrior.....	27
Figure 10	The Battlefield Network	31
Figure 11	Single Points of Failure	36
Figure 12	Eliminating Single Points of Failure	37
Figure 13	FDDI Isolating a Failed Node	39

EXECUTIVE SUMMARY

The purpose of this thesis is to introduce the concept of having a jointly integrated network to better enhance battlefield communications and the dissemination of information using a smart push/pull concept from the highest commander down to the individual soldier. The concept of having a robust and dynamic network could provide the United States Armed Forces a better way of integrating the individual soldier's performance into higher level units. With such a system, every member of the battlefield would have access to critical information in near real time. Each service could purchase any new data system or datalink, and connecting it to the network would mean that anyone on the network could access any of the information that the new system carried. The net-centric concept relies heavily on systems engineering concepts and steers away from the conventional stovepipe systems commonly found throughout the services. Relying on stovepipe systems hampers the services' abilities to work together in a joint operation. The implementation of a battlefield network would better enhance joint operations and interoperability. The current communications systems in use today by the services are not interoperable with each other. They require specific equipment that not all units have in their inventory.

The battlefield network would help in the achievement of the C4 systems objectives as set forth in Joint Pub 6-0. It would also meet most of the doctrinal requirements laid out in Joint Pub 6-0. The key to the battlefield network would be to take a net-centric approach. The net-centric approach is to have the network as the central part in the command, control, and communications

structure on the battlefield. Having the network being the center of the structure, it will be easier to make the single network hardened than hardening many different networks. The net-centric approach would provide connectivity throughout the battlefield. As systems enter the battlefield they could be simply hooked up to the network. The net-centric approach allows the network to grow as the need arises. This approach also allows the integration of COTS and GOTS equipment to meet the needs of the commands on the battlefield. With the network as the center of the communications between end systems, the interface between the end system and the network can be defined by open standards. The net-centric approach allows for the start of internetworking the existing stovepipe systems.

With a networked battlefield the common global vision as set forth in Joint Pub 6-0 and C4I For The Warrior would be achieved. The sensor-to-shooter concept would also be realized with the inception of a battlefield network. True force interoperability could be achieved through mutual cooperation of service components in the theater. The interoperability between the services today is lacking in many respects and could benefit from a battlefield network. The network would allow all of the services to share information in a more dynamic way than can be achieved today.

The battlefield network must meet some standard baselines which include: the capability of incorporating radio, cellular, LAN and WAN networks; adherence to standards that have been tested in the commercial world of networking; an end system must be able to plug into the network at any time or

place; the network must be easy to set up and maintain; the network should have high availability, reliability, and survivability built into it; and the network should incorporate COTS and GOTS equipment where appropriate. The network should also have a flexible backbone for scalability purposes. The network should be flexible enough to support any number of forces.

End systems, sub-nets, and network devices should meet the specific requirements of the OSI layers. With these OSI layer ingrained in all networks that will comprise the battlefield network, the connection of these networks will be simplified, thus making them, as is referred to in the commercial world, plug and play. If current systems cannot be adapted to conform to IP and the OSI model, then they should be replaced by systems that meet this requirement. Current networking COTS and GOTS equipment are available that meet these requirements. Other end systems, such as radars, should have network compatible LAN, logical, and management interfaces built into them so that they can be easily integrated into the network. A good network management system has to be used to monitor the network due to the nature of the network and the information carried on it.

Overall, this network could be built today for our forces in the near future. The armed forces could have a network that would meet their needs of today as well as their needs of tomorrow. Cooperation among the services is needed to accomplish this goal. Through cooperation the services will bring the interoperability for today's and tomorrow's joint operations.

ACKNOWLEDGEMENT

The author wishes to thank Professors Dan Boger and Rex Buddenberg for their patience and guidance during this effort. The author also wishes to thank Jean, Christopher, and Zackary without whose patience, understanding, and support this effort could not have been accomplished.

I. INTRODUCTION

A. PURPOSE OF THESIS

The purpose of this thesis is to introduce the concept of having a jointly integrated networking schema to better enhance battlefield communications and the dissemination of information using a smart push/pull concept from the highest commander down to the individual soldier. The concept of having a robust and dynamic network could provide the United States Armed Forces a better way of integrating the individual soldier's performance. With such a system, every member of the battlefield would have access to critical information in near real time. Each service could purchase any new data system or datalink, and connecting it to the network would mean that anyone on the network could access any of the information that the new system carried. This would save untold money and limit the need for stovepipe systems. The network-centric concept relies heavily on systems engineering concepts and steers away from the conventional stovepipe systems commonly found throughout the services. Relying on stovepipe systems hampers the services' abilities to work together in a joint operation. The process of sharing information between the services becomes quite difficult if that information is passed over service-specific devices. This increases the time required to share critical information. The information, once received, would not be up to date and could cost time and lives depending upon the content of the information. In a networked battlefield, information, data, graphics, or national

sensor information could be shared in near real time to anyone who would have a need for that type of information.

The network-centric approach would encourage the services to cooperate more in acquiring joint systems that would have the capabilities needed by all of the forces. For service-specific requirements, the services could port some of the data that other battlefield components need to the network. This would ultimately save money on the purchasing of hardware and software. The requirements placed on the network would be commonality of components (data and protocols). The different services would have to agree on these common components. In order to save money on implementation one would only have to look at the availability of products that are currently out in industry. By using proven networking systems, the services could have a network structure for far less money than using current service-specific, mission-specific stovepipe systems. By looking at the functionality of the Internet, one could only imagine what could be achieved in the battlefield of the future.

B. BACKGROUND

Since the beginning of armed conflict, history has shown that commanders found the need to improve communications down to their respective troops. Commanders of our past used instruments (drums, bagpipes, horns), flags, lighting devices, messengers, etc., to signal troops and subordinate commanders to execute their standing orders. With the inventions of this century, the job of communicating to respective subordinates has grown easier on both sides.

Therefore, the possibility of a battle happening after peace has been declared, as happened in the War of 1812 with the Battle of New Orleans (the Senate had yet to ratify the peace treaty) [Ref. 1], is unlikely to happen in today's environment.

However, there has been and always will be a need to pass critical information up and down the chain of command. In today's battlefield environment the passing of this critical information could be better enhanced using existing technologies. With the complexity of today's battlefield, the need for this information increases exponentially with the destructive power being placed in the common soldiers' hands. A platoon soldier armed with a grenade launcher and machine gun can level a building in a matter of minutes. A pilot with a standard load of iron bombs or a couple of smart weapons could level a platoon, building, or other large targets.

Friendly fire casualties are of great concern to everyone. Without critical information, close air support missions could be disastrous. If the pilots are not informed of updated positions of friendly forces, the potential is there for friendly fire incidents. Current communications are not good enough to provide the position updates fast enough. With the use of networks, this position updating could occur in near real time. Airborne assets would see the position updates of friendly troops in graphical form on their displays. This would increase their situational awareness. Artillery units could also benefit from the use of networks and near real time information that would be provided on friendly and enemy positions. Friendly fire incidents have cost many unnecessary deaths in past wars

such as World War I, World War II, Korea, Vietnam, and Desert Storm. Now with the introduction of networks to pass data using the push/pull concept these incidents could be severely curtailed.

C. SCOPE

This thesis is intended to provide a concept of how using layered networks could greatly improve the conduct of the art of war by Armed Forces of the United States. Also, the armed forces could benefit from this concept due to reduced spending on costly systems that are currently in inventory. Information collected from current systems could be shared throughout the battlefield with those who need the information. The capability of implementing this system could be quickly set up and would provide robust communications using current off-the-shelf technology and current hardware that is in inventory. The networking concept would produce commanders and soldiers with an untold wealth of information that would be time critical and could potentially save many lives, plus it could help in defeating enemies quickly.

The networking concept could change the command hierarchy in the battlefield. The concept would flatten the command hierarchy structure in the battlefield. At present the command hierarchy is more top down; it resembles a tree. This would have to be looked at in future studies to determine what kind of doctrine would be needed. It should be noticed that the command hierarchy is flattened by the phone system when units are in the United States. In theory any soldier could pick up the phone and dial the number of the commander higher up

in his chain of command. That is also true of the commander dialing up the lowest soldier under his command and giving him a direct order. This would also be possible if a network system is implemented for the battlefield. Although the possibility exists, the author believes this would not happen due to the same restraints that service members use when located in the United States.

II. CURRENT TACTICAL SYSTEMS

A. OVERVIEW

This chapter will discuss current ways the military uses to get critical information to the warfighter in today's battlefield environment. The following systems will be discussed: datalinks, voice communications, and the global broadcast system.

B. LINK-11

Also known as TADIL A, Link-11 is a netted, two-way, real time, encrypted datalink which uses half duplex HF and UHF communications circuits for computer-to-computer data interface to pass track information management data, command and control information, and status data among up to 20 Navy, Marine Corps, and Air Force participants, Link-11 uses a star net topology (Figure 1) with discrete transmit but full receive

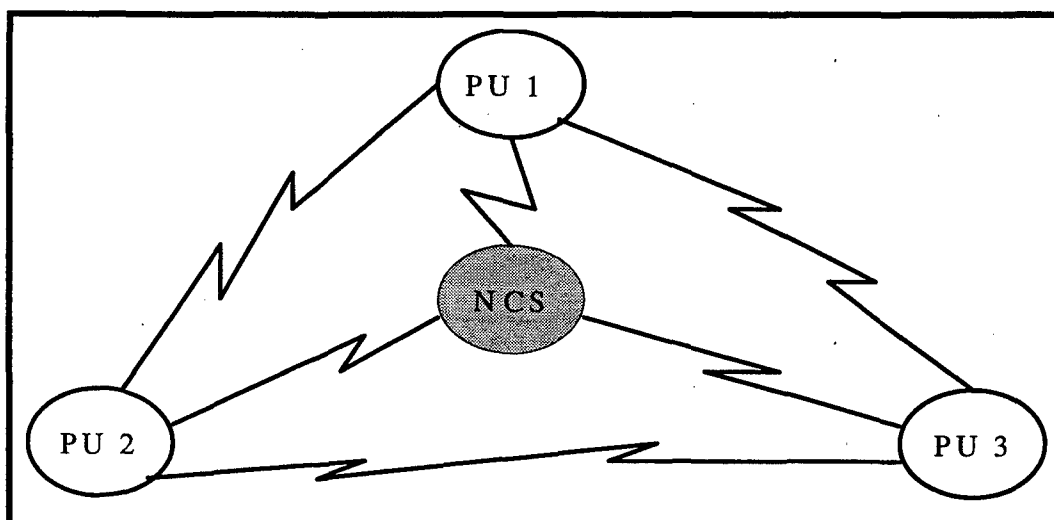


Figure 1 Link-11 Star Topology

connectivity [Ref. 2]. Link-11 uses a polling protocol and a netted architecture. A net operates under a net controller which permits participant access and is responsible for circuit discipline. In its normal operation, Link-11 is normally operated in Roll Call mode. Participating Units (PUs) transmit all reportable data when polled by the Net Control Station (NCS). Once a PU transmits it switches to receive mode. The NCS then polls the next PU in its list. Figure 2 shows how the polling method works with different PUs. In current terminology, Link-11 is a token broadcast. This continues until all of the PUs have transmitted their data. The process is then repeated continuously. The time for all PUs in the net to be polled and transmit their data at least once is called the net cycle time. The goal of the NCS is to keep the net cycle time down. If net cycle time is large then the NCS may drop one or more PUs off the net.

Link-11 uses M-series messages. The messages are made up of two 24-bit frames. At the fast data rate Link-11 is capable of handling 1800 bits per second. With error detection and correction enabled Link-11 is capable of transmitting 2250 bits per second with 6 bits of each frame (30 bit frame, 24 bits for data word, 6 bits for encoding) being used for the error detection and correction [Ref. 3].

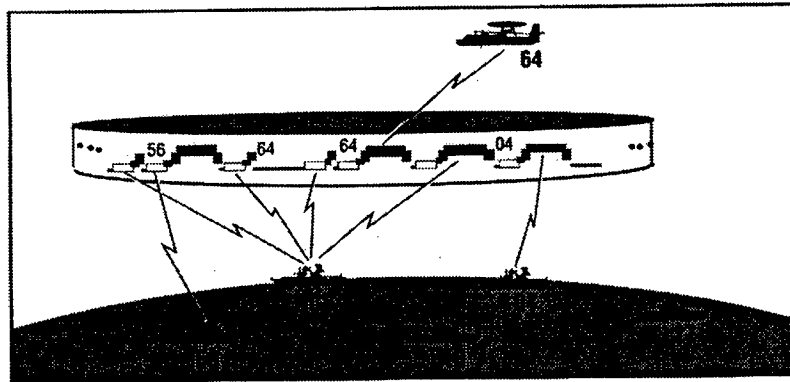


Figure 2 Link-11 Polling From Ref. [4]

There are many different configurations for Link-11 depending upon the platform. A generic configuration is represented in Figure 3 [Ref. 5]. The tactical data system computers have two main Link-11 functions. They supply tactical digital information to net participants and retrieve and process incoming tactical digital information received from net participants. The Key Generator-40 (KG-40) is an encryption device. The Data Terminal Set (DTS) converts the data from a digital format to an analog audio signal on outgoing data and in the reverse order for incoming signals. The last component is either an HF or UHF radio.

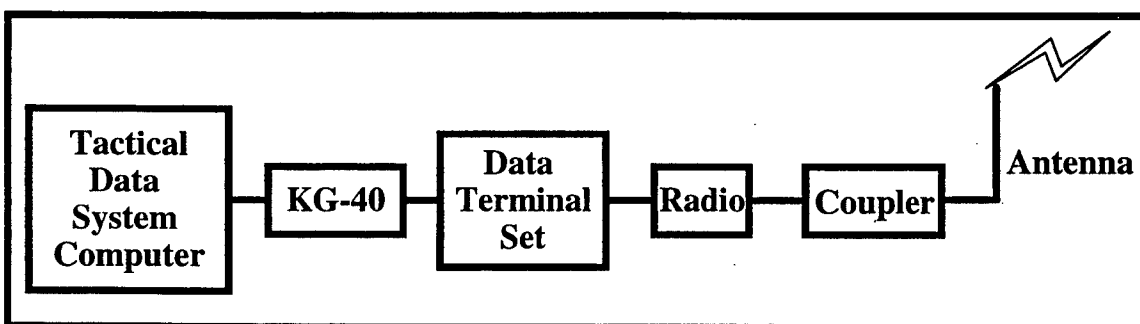


Figure 3 Link-11 Components After Ref. [5]

C. LINK-4A

Link-4A, also known as TADIL-C, is an aircraft control data link. It normally interconnects tactical and support aircraft to an aircraft control unit typically to support air intercept operations. Link-4A is a half duplex digital data transmission system used to transfer aircraft control and target information between a control station and a controlled aircraft. It uses a command-and-response protocol along with time division multiplexing. This combination derives an apparently simultaneous channel from a single frequency. The aircraft controller circuit is in basic form a point-to-point circuit. Figure 4 shows a typical Link-4A net.

The Link-4A messages are either control messages or aircraft reply messages. The control messages are known as V-series messages, and the aircraft reply messages are known as R-series messages. The controller sends a 56-bit control message every 32 msec, for a one-way tactical data rate of 1750

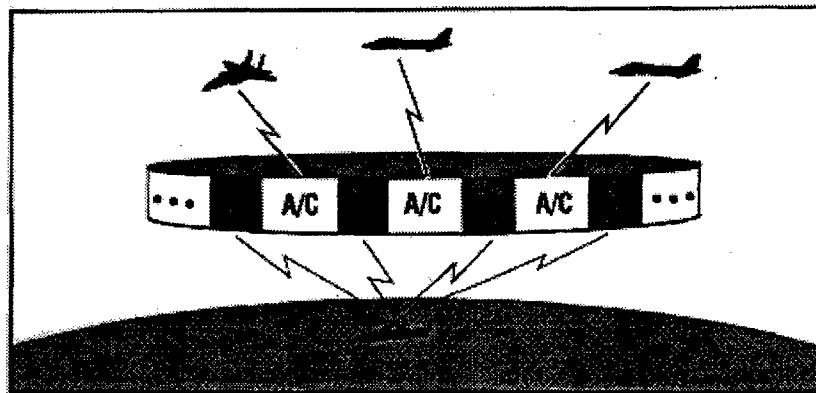


Figure 4 Link-4A Net From Ref. [4]

bits per second. The effective two-way tactical data rate is approximately 3000 bits per second. Link-4A does not use parity or error detection and correction [Ref. 4]. Figure 5 is the typical equipment configuration for surface platforms [Ref. 6].

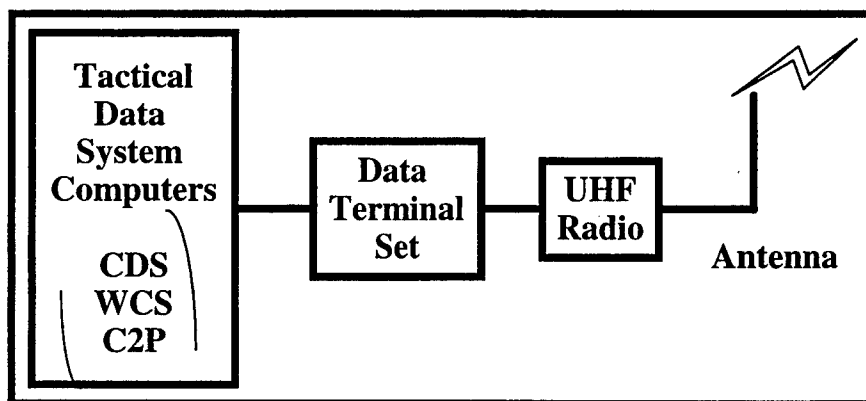


Figure 5 Link-4A Equipment Configuration From Ref. [6]

Link-4A is used for other missions besides air control. They are as follows: air traffic control (ATC), automatic carrier landing system (ACLS), carrier aircraft inertial navigation system (CAINS), and strike control (STK). ATC is simply precise direction of air traffic within a given area. ATC is often used in conjunction with ACLS to bring controlled aircraft to a location at which the ACLS may take over and guide the aircraft to landing. ACLS is designed to automatically guide aircraft down to landing, day or night, either on the deck of a carrier or onto an airfield, during the final approach and landing. ACLS operates in either automatic or semiautomatic modes. The automatic mode provides direct control to a landing. The semiautomatic mode provides the pilot with visual indication of the path to fly in order to land. CAINS is the capability through Link-4A to align the inertial navigation systems of aircraft with the aircraft carrier. This typically occurs on deck before a flight. STK is the directing of aircraft to surface targets in order for the aircraft to attempt to destroy those targets.

D. LINK-16

Link-16 (TADIL-J) was developed to support the Command, Control, Communications, and Intelligence function in multiservice and Navy battle group operations [Ref. 7]. It uses Joint Tactical Information Distribution System (JTIDS) terminals along with the computer systems of the units. Figure 6 pictorially represents this makeup. Link-16 fills the deficiencies of the existing data links. It uses a Time Division Multiple Access (TDMA) protocol to increase its capacity over other data links. By using TDMA, Link-16 has 30 times the capacity of Link-11 [Ref. 7]. The highest data rate of a single terminal is 54,000 bits per second. However, since TDMA and the division of timeslots are used the overall system rate is much higher. The effective data rates of Link-16 are 26,880, or 53,760, or 107,520 bits per second, depending on which type of data packing structure is being used. Link-16 uses J-Series messages.

Link-16 has the capability to stack different nets. Figure 7 depicts a stacked Link-16 net. Multiple nets can be stacked by allowing time slots to be used redundantly, with the data transmitted in each net on different frequencies. There are 51 frequencies available for transmissions. The frequency is not held constant during each time slot but is changed rapidly (every 13 microseconds) according to a predetermined pseudo-random pattern. This pattern is a fast hopping spread spectrum pattern. Each net is assigned a number which designates a particular hopping pattern. There are 128 possible numbers, with the number 127 reserved to indicate a stacked net configuration. During any given time slot, a unit

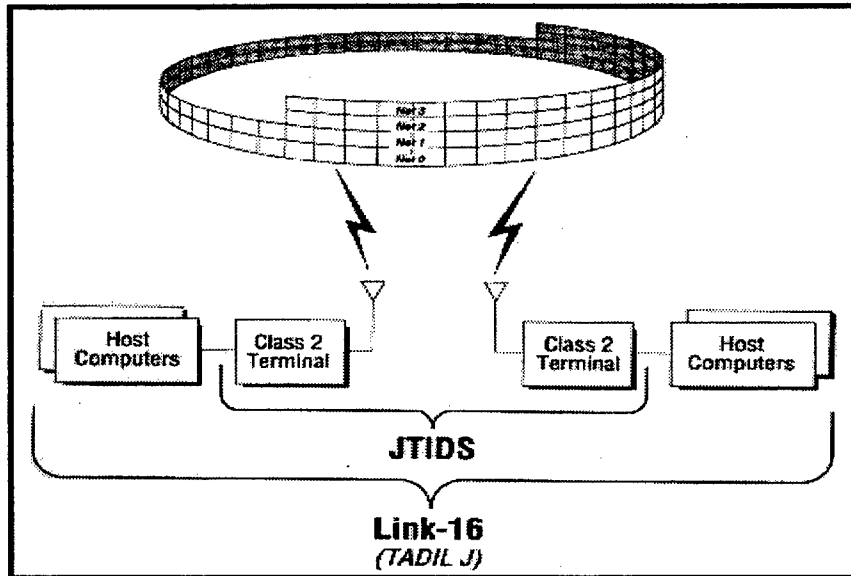


Figure 6 Link-16 System From Ref. [4]

is either transmitting or receiving on one of 127 possible nets. Although in theory there are 127 total possible nets, analysis has shown that approximately 20 different nets can be co-located without mutual interference [Ref. 4].

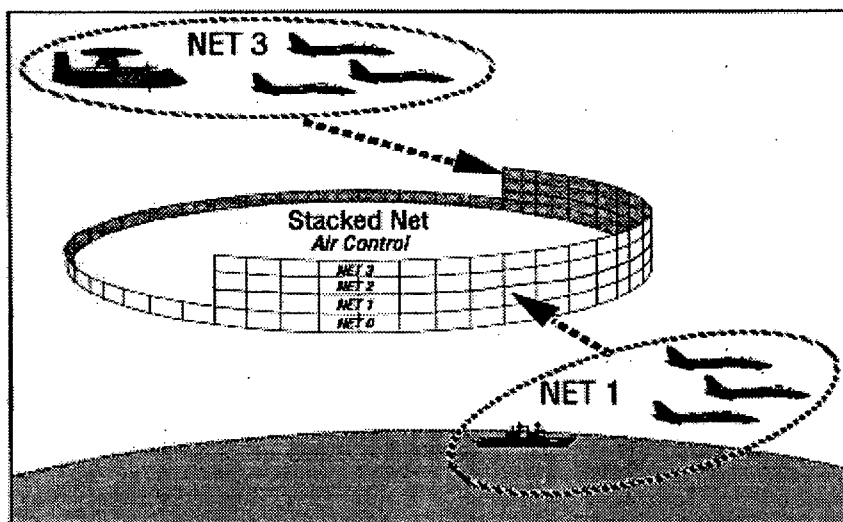


Figure 7 Link-16 Stacked Net From Ref. [4]

For security of communications, each JTIDS terminal is equipped with a Secure Data Unit. The Secure Data Unit provides for message and transmission security. Each message is encoded at transmission with a unique transmission security crypto variable. This variable establishes a hopping pattern and pseudorandom noise encoding. Each transmission is also data encrypted to provide message security prior to transmission. A further enhancement to security is the combination of the pseudo-random hopping patterns, TDMA, and the way that the messages can be formatted. This combination provides randomness and complexity further preventing an enemy from gaining information that is passed over a Link-16 net [Ref. 7].

Link-16 operates in the 960-1215 MHz range. This normally produces line-of-site connectivity; however by using relaying units, connectivity can be provided to units beyond line-of-sight. The TDMA propagation time limit determines the maximum point-to-point range. JTIDS point-to-point connectivity by line-of-sight is less than 300 nm. This range can be extended to approximately 500 nm using relays. These relays are akin to bridges and repeaters in a network.

Link-16 tracks incorporate all Link-11 tracks, plus it is capable of reporting land tracks. It also has the capability of unit identification which includes platform, activity, specific type, and nationality. It also incorporates an identity of Neutral. Friendly aircraft can report equipment status, exact ordnance inventory, radar and missile channels, fuel available for transfer, gun capability, and ETA and ETD to or

from station. The capability of reporting areas and lines has been enhanced over the current capabilities of the Link-11 system.

Link-16, Link-11, and Link-4A all rely on different message formats. For this reason they are not very flexible. This problem, among others, would have to be fixed in order for them to be integrated into a network environment. Link-16 also relies on a JTIDS terminal for its interface. For use in a network environment this would have to be corrected also.

E. GLOBAL BROADCAST SYSTEM (GBS)

GBS is a new application based on the popular commercial Direct Broadcast Service (DBS). GBS has a high data rate up to 23 Mbps and a small receive antenna. The concept of GBS is to provide secure simultaneous broadcast of data to a theater of operations, world-wide coverage from 70°N to 70° S, and use commercial-off-the-shelf (COTS) equipment. It should have the capability to transmit data at all classification levels from unclassified to SCI. GBS will use the asynchronous transfer mode (ATM) for its switching technology. The GBS concept of operations provided the following [Ref. 8]:

- provide for two modes of operation: wide area coverage and steerable "spot beams."
- provide three classes of tailored service: continuous, periodic, and on-demand.
- maintain interoperability with IP-based addressing schemes.
- augment current MILSATCOM systems.
- use Global Command and Control System (GCCS) as the primary interface for service requests.

- transmit data from CONUS uplink sites while allowing in-theater (CINC-responsive) injection of data.

Currently there are no military MILSATCOM communication systems optimized for GBS. Currently there are plans to place transponders aboard the last four of the US Navy's Ultra High Frequency Follow-On (UFO) satellites. This will allow each UFO satellite to have two steerable spot-beams (500 nautical mile diameter coverage each) operating at 24 Mbps, one wide area (200 nm) GBS broadcast operating at 1.544 Mbps, and an uplink accessibility from at least one (of four) NCTAMS site at all times. Initial GBS operational capability is slated for the first quarter of 1998. However, there are fourteen US warships with DBS commercial systems. There are also theater level GBS systems being used in the US for testing and supporting US and NATO Forces in Bosnia. As the capabilities evolve, operations and capabilities of GBS will be expanded.

F. VOICE COMMUNICATIONS

Voice communication has been the mainstay of military communications. A majority of information transferred to the shooter today is carried out over voice nets. Voice communications does have its place on the battlefield but does at times cause confusion and does not always provide the picture needed to enhance situational awareness. Commanders typically use voice communications to tell their troops what to do and how to carry out their mission. A majority of air control is carried out by two-way voice communication. Datalinks have eased the need to report everything by voice, but some datalinks use voice for net control.

Various types of radios are used to carry out this communication. Cellular phones have also made their way into military use. This technology has many promises for future use. It can be used for voice transmissions, and when a modem is attached it works great for transmitting data over the circuit. The Army is buying the SINCGARS radio which is a great tactical voice radio but has a limited data capability. Advertised digital data rates from General Dynamics technical specifications sheet are 600, 1200, 2400, 4800, and 16,000 bits per second using frequency shift keying [Ref. 9]. The SINCGARS radio operates in the 30 to 87.975 Mhz range [Ref. 9]. It also has a frequency hopping capability which makes it harder to jam and have its transmissions intercepted. Overall, voice communications is still needed in some areas, but in other areas it could be replaced with data communications that could offer the shooter more information in less time.

G. SUMMARY

This chapter has focused on some of the current systems that are used in the military for passing information. These systems are not interoperable with each other due to their different messaging formats. The information that all of these systems pass should be available to everyone who needs that data without having to have specific equipment. Link-16 is the newest data link in the system but not everyone will have access to the information passed over it due to the cost of the hardware required.

The data links in their current form are not compatible with a network environment. The compatibility issues will be discussed later in this thesis. In the next chapter the basic objectives and doctrine for a C4 system will be discussed along with a network concept that can be applied to the battlefield. Some of the systems discussed in this chapter could be integrated into a network with ease while others would need major modifications.

III. OBJECTIVES AND DOCTRINE

A. C4 SYSTEMS OBJECTIVES

Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6-0), sets forth fundamental objectives that a C4 system has to meet. These objectives are [Ref. 10]:

- **Produce Unity of Effort.** C4 Systems should help a military force and its supporting elements to combine the thoughts and impressions of multiple commanders and key warfighters. This allows the views of many experts to be brought to any task.
- **Exploit Total Force Capabilities.** C4 systems must be planned as extensions of human senses and processes to help people form perceptions, react, and make decisions. This allows people to be effective during high-tempo operations. C4 systems must be immediately responsive, simple, and easily understandable.
- **Properly Position Critical Information.** C4 systems must be able to respond quickly to requests for information where it is needed.
- **Information Fusion.** The ultimate goal of C4 systems is to produce a picture of the battlespace that is accurate and meets the needs of warfighters. This goal is achieved by fusing information and putting it in a form that people can act on. With concise, accurate, timely, and relevant information, unity of effort is improved and uncertainty is reduced, enabling the force as a whole to exploit opportunities and fight smarter.

Unity of effort, as defined by Joint Pub 1 [Ref. 11], starts at the national level with the national security strategy which employs the political/diplomatic, economic, informational, and military powers of the nation to secure national policy aims and objectives. The Chairman of the Joint Chiefs of Staff (CJCS) along with the other members of the Joint Chiefs of Staff (JCS) in turn make the national military strategy to provide focus for the US military. When a crisis breaks out the

combatant commander in charge of that region is normally supported by other combatant commanders, and federal agencies, thus focusing the unity of effort to that crisis. Unity of effort transcends time and technology, but in today's environment unity of effort is supported in this endeavor by technology. The battlefield network can help in this unity of effort. Information from other combatant commanders, JCS, and federal agencies could pass over connections to the network where it can then be distributed throughout the battlefield. The subnets bringing that information in could also be used for communications with supporting combatant commanders, JCS, and federal agencies to help the local combatant commander solve difficult problems.

The network also allows exploitation of total force capabilities by providing commanders a total battlefield picture. The forward troops provide the commanders with the information of the battlespace that surrounds them, much like the fingers on a hand. The national systems sensors provide more information about the battlefield. With all of this information a battlefield picture is formed and the commanders can make decisions, react to the changing battlefield, and disseminate their orders quickly to subordinate commanders. Equally as important, lower echelon commanders could pass information up the chain of command concerning actions that they have taken on their own initiative. Critical information would be within easy reach of everyone who needed that information in a networked environment. Distributed databases would allow warfighters to pull information that they needed in order to make more informed

decisions. The network could not itself fuse the information but could pass the fused information quickly throughout the network to battlefield commanders.

B. BASIC DOCTRINE FOR C4 SYSTEMS

For a C4 system Joint Pub 6-0 puts forth some basic doctrine that any system has to meet. This doctrine is inherent in a network. They are as follows [Ref. 10]:

- **C4 Systems must provide the rapid, reliable, and secure flow and processing of data to ensure continuous information exchange throughout the force.** An unbroken chain of communications must extend from the National Command Authorities (NCA), through the Chairman of the Joint Chiefs of Staff (CJCS), to the combatant commanders, commanders of Service components, and all subordinate commanders.
- **Operations, logistics, and intelligence functions all depend on responsive C4, the central system that ties together all aspects of joint operations and allows commanders and their staffs to command and control their forces.**
- **C4 systems provided to combatant commanders operate under their authority and will be an integral part of their C2 infrastructure.**
- **Joint Force Commanders (JFC) must develop operational procedures that provide interoperable, compatible, C4 networks.**
- **The complexity of joint operations and the finite amount of C4 resources may require the JFC to adjudicate or assign subordinate command responsibilities for providing C4 systems support.**

The preceding doctrine are goals for a C4 system. However, these goals are not currently met. The second basic doctrine listed concerns operations, logistics, and intelligence functions. Currently separate systems are used to support these functions. With a battlefield network, these functions would be

carried out on the same infrastructure. This would eliminate the need to have separate systems.

One problem with this basic doctrine lies in the portion that C4 systems provided to combat commanders operate under their authority. This portion of the doctrine is a prescription for stove-piping systems. Networks do not inherently subscribe to this philosophy. Networks, by nature, are expansive because of the widely varying interoperability needs of the network. The network would also have resources outside of the combatant commander's control. Some of these resources outside the commander's control would include national sensors, databases maintained by national agencies, and other information sources or sensor platforms. A network by its nature is more adept at fitting into a flattened command structure than a hierarchical structure. In a network environment, personnel do not have to rely on commanders to supply information to them. They can go to the source on the network and pull the information to them. The network provides connectivity to everyone. This is one reason that a network supports a more flattened command structure. However, a network can be structured to support a hierarchical command structure, but this is more of a doctrinal issue than it is a network issue. Thus this portion of doctrine should be examined for networks, especially for a battlefield network.

A battlefield network will provide a reliable means for passing information throughout the battlefield forces. Through connectivity with sub-networks that extend from the United States to the battlefield, the NCA and CJCS can

communicate to the commanders on the battlefield. This would be inherently built into the network through its design. The network would be able to accommodate network traffic from the support personnel from all services. The reordering of supplies and requests for intelligence data could easily pass through the network and reach its destination quickly. This is due to the connectivity of the network. The interoperability and compatibility will be built into the network. The equipment brought into the battlefield by components will be a part of the C2 infrastructure. Each battlefield unit will be able to bring their equipment and hook into the network. This will solve many issues that are now faced in the battlefield environment. These include compatibility, interoperability, and the ability to share information.

C. NET-CENTRIC CONCEPT

As the armed forces approach the next century, the weapon systems that are being put in use are more complex and deadly. The sensors used to target these weapons are providing more information than those of the past. The way that data is provided throughout the battlefield has also changed, but it has not kept up with technology and commercial world solutions to pass the data.

The key to the battlefield network would be to take a net-centric approach. The net-centric approach is to have the network as the central part in the command, control, and communications structure on the battlefield. Having the network being the center of the structure, it will be easier to make that single network hardened than hardening many different networks. By having the network

in the center of the structure it will be more important to harden this network. The network's design should be such that provisions for availability, reliability, and connectivity be built in throughout the battlefield. Initially this will be expensive to do but will pay off in the end. By paying attention to the details of the design the network will be more survivable and meet the needs of the armed forces. This would also provide more robust data sharing.

Current communication systems would be connected to the network. Figure 8 is a pictorial view of the net-centric concept. The network is in the center of the battlefield command, control, and communications system.

- The net-centric approach provides connectivity throughout the battlefield.
- Additional systems that are brought into the battlefield could be simply hooked up to the network.
- As new systems are built they would have to include connectivity and data sharing capability with other systems that connect to the network.
- A net-centric approach allows the network to grow as the needs arise.

This approach also allows the integration of COTS and government of the shelf (GOTS) equipment to meet the needs of the commands on the battlefield. The integration is a benefit of the net-centric concept. With the network as the center of the communications between end systems, the interface between the end system and the network can be defined by open standards. Each end system that is connected to the network would have to be looked at individually to see what can be bought commercially to interface with the network and what would

have to be built specifically for that system to interface with the network and meet the open standards.

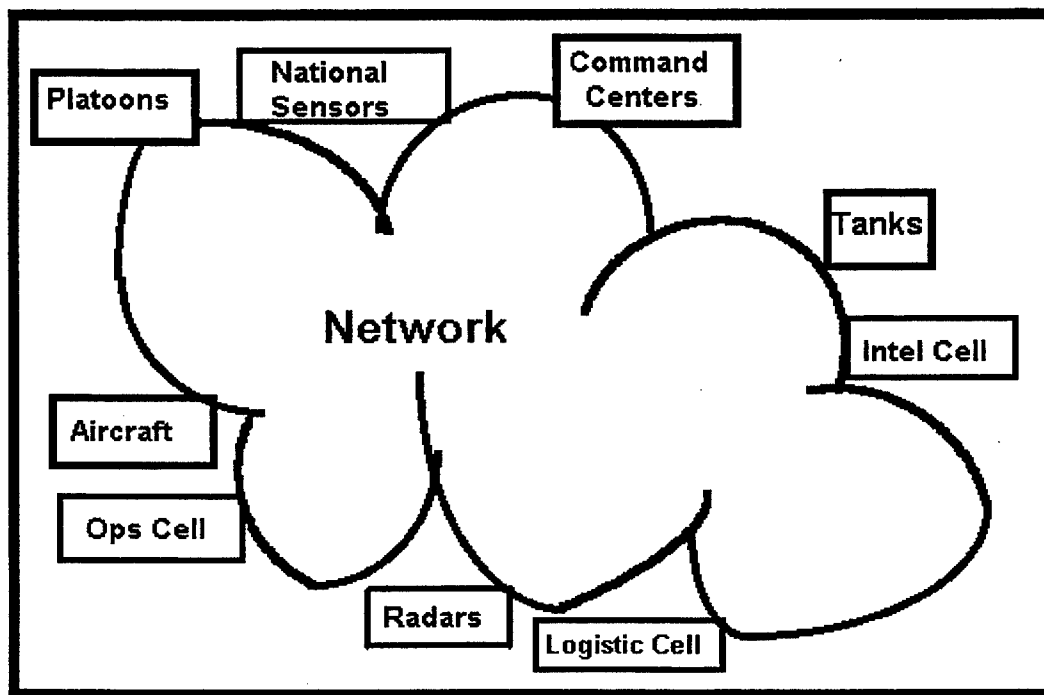


Figure 8 Network Subsection After Ref. [13]

With the increase in the development of computer and networking technologies in the past few years, the time has come for the armed forces to start internetworking the existing stove-pipe systems. The net-centric approach is one way to achieve this integration.

Our enemies in the future will have access to the same computer and networking technology that is available to our armed forces. Some of these enemies will have their information systems networked providing them with shared information. These same enemies may also share the same infrastructure for data transmission as our armed forces. Our armed forces' and our enemy's data

could pass over the same satellite and telephone lines. This would present a great problem in that you could not take down the enemy's datalinks as it would affect our armed forces' data that passes over the same links. As more dual use technology (such as cellular satellite services, internet connectivity, and telephone lines) becomes available world-wide, more countries' armed forces will use this technology. Our armed forces will use this technology for communications and our allies will use this technology in theater.

D. BENEFITS OF A BATTLEFIELD NETWORK

With a networked battlefield the common global vision as put forth in Joint Pub 6-0 and C4I For The Warrior would be achieved. Figure 9 is from Joint Pub 6-0 [Ref. 10]. It is the evolution of C4I for the Warrior in a pictorial view. This shows the migration from WWMCCS to GCCS and the extension of that to the battlefield. Another benefit of a battlefield network is that the sensor-to-shooter concept would also be realized. Sensor information is on the network. In some cases this data would have to be fused for the upper echelons of command. This would help give the higher commanders the battlefield picture without showing every platoon member's position, but a symbol of the platoon's position would be shown instead. As the relevant command descends the organizational hierarchy, the positions of each platoon member would become more important. Before shooters would be allowed to shoot at a target, the Command and Control (C2) node, which is also connected to the network, would prioritize the targets before

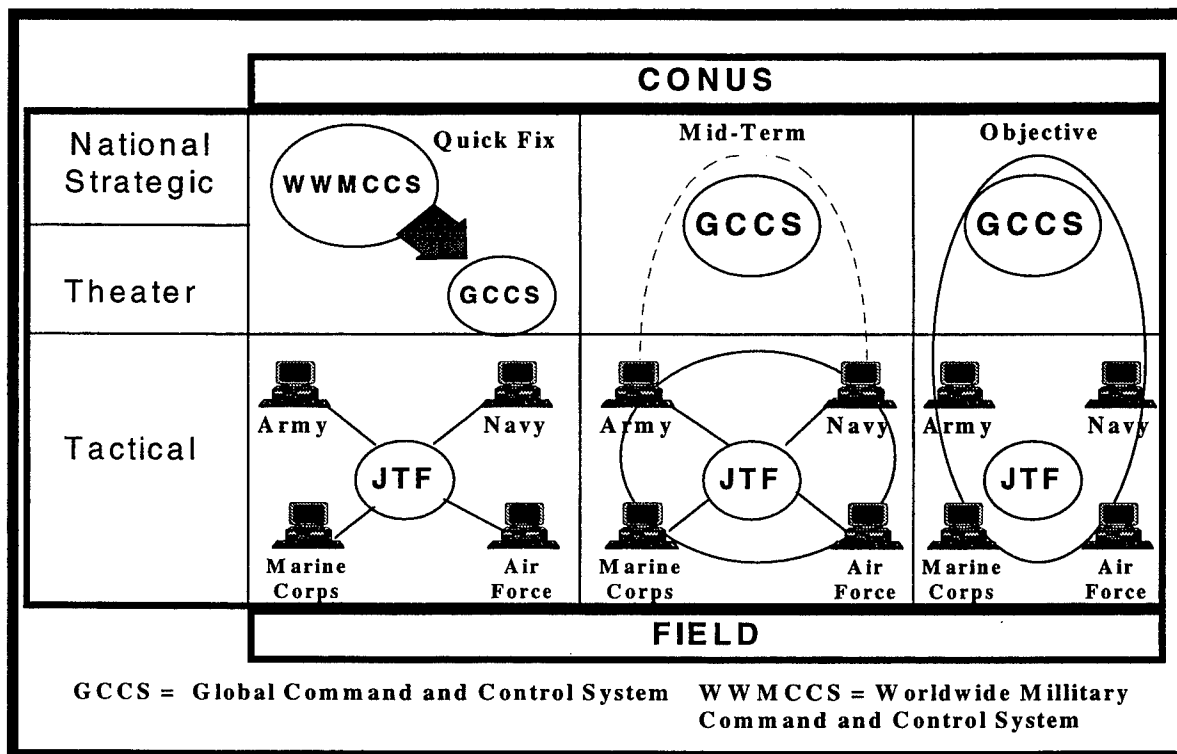


Figure 9 The Evolution of C4I for the Warrior After Ref. [11]

authorization is given to take out a target. The prioritization by the C2 node is more of a doctrinal issue than it is a network issue. The C2 node can add discipline, but positive control or control by negation is a matter of doctrine and the rules of engagement (ROE). The C2 node could reduce the instances of using weapons on secondary targets before hitting the primary targets. For some of the ground shooters, sensors reporting enemy ground forces would give much better situational awareness to those shooters.

By having a networked battlefield, true force interoperability could be achieved through mutual cooperation of service components in the theater. The network would allow all of the services to share information in a more dynamic way than before. Intelligence cells from all services could share information quickly

from different parts of the battlefield to form a battlespace picture of the enemy and friendly positions. The Air Tasking Order could be disseminated to everyone no matter what system they are using by sending it over the network. Force integration could be used by the Joint Force Commander (JFC) to achieve an objective. The JFC could disseminate his orders to subordinate commanders swiftly. In turn, those subordinate commanders would then be able to further make decisions and pass their orders down the chain of command until those orders are executed. Overall, the network battlefield would allow quicker sensing of the battlefield, more informed decision making, and faster actions based on those decisions.

The discussion in this chapter has focused on the objectives and basic doctrine of a C4 system, the net-centric approach and the benefits of a networked battlefield. The evolution of networking the battlefield will happen eventually as the benefits of networking become apparent to all members of the military. An approach to building the battlefield network will be offered in the next chapter.

IV. THE NETWORK VISION

A. THE BIG PICTURE

The following lists of bulleted items lay the baseline for a battlefield network.

- A battlefield network must be able to incorporate radio, cellular, LAN and WAN networks.
- Using commercial standards in the network would be a big benefit to DOD, because these standards could be proved and improved upon in the commercial market first before being incorporated into the battlefield network.
- These standards decided upon would have to be in use in the commercial world. This would make sure that they are tested before they are used in the battlefield network, thus saving DOD the cost of development and testing.
- A side benefit of using commercial products is that they tend to be more user friendly than strictly military-developed products.
- Any end system must be able to plug into the network at any time or place.
- The network should be capable of carrying any kind of data from email to imagery and tactical track data that is currently carried in current tactical data links.
- The network should be easy to set up and maintain.
- This network should have high availability, reliability, and survivability built into it.
- The network should incorporate COTS and GOTS equipment where appropriate. By using commercial products, where appropriate, the Department of Defense (DOD) could target research and development funds on the parts of the network that would have to be developed rather than reinventing the already available parts.

The terms "end system" and "sub-net" will be used throughout this section. An end system is any system that produces or consumes data. A sub-net is connected to an end system and passes data through it. Sub-nets can be internetworked. A sub-net can be considered as a transmission pipe. Some examples of end systems are aircraft, command centers, and platoons. Examples of sub-nets are current tactical data links (Link-16, Link-11, Link-4A), Mobile Subscriber Equipment (MSE) nets, GBS, and current radio networks.

Figure 10 shows a portion of the envisioned network. As more units enter the battlefield they could simply plug into the network. The network could start out as a radio WAN, and as non-mobile units enter the battlefield, a terrestrial WAN could be set up to accommodate those units and meet the high traffic needs.

In Figure 10 there is a mix of different components that make up the battlefield network. This figure is the second layer down from Figure 8. What is not represented here is the mobile forces that move from one point in the network to another. An example of this would be an aircraft that is initially hooked into the ship's LAN and after takeoff plugs into another section of the network. Another issue that this figure cannot represent is the security that is inherently involved in a military network. Also network management compatibility is not represented.

On the other hand Figure 10 does show a good user perspective of the battlefield network. There are numerous ways to connect to the network. The LAN on the left side could be a logistics or intelligence cell that has connectivity through the terrestrial WAN to the rest of the network thus allowing passage

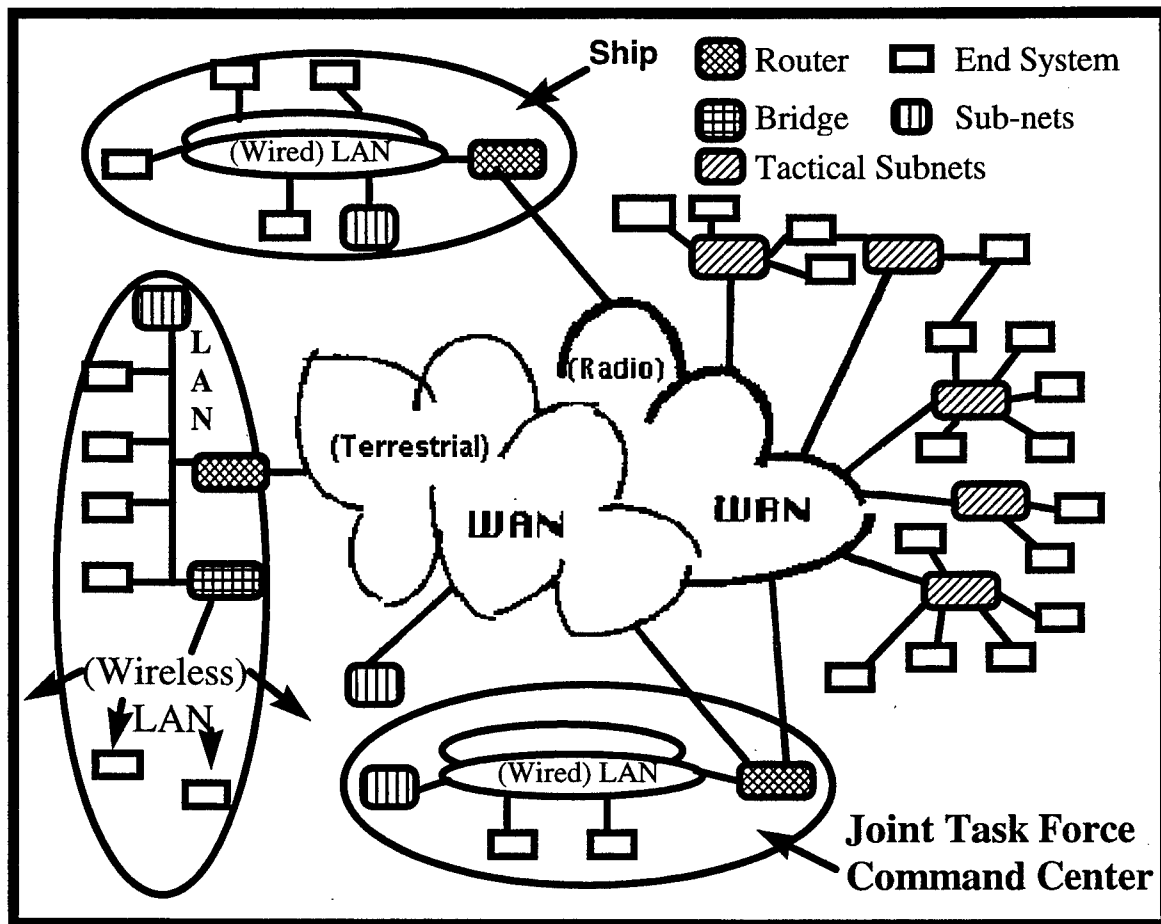


Figure 10 The Battlefield Network After Ref. [13]

of data throughout the battlefield. The ship also has connections to the network via a router hooked into the radio WAN. This would allow direct connectivity to the units who need the firepower that the ship can provide. The Joint Task Force command center has connectivity through the network so that dissemination of orders and gathering of information can easily happen. The Joint Task Force command center could also pass information that is resident on GCCS to the rest of the battlefield if the need arises.

The overall structure of the network is not known before forces arrive in the theater. As forces arrive into the theater the network would grow. Individual units

would have to bring in their equipment to hook up to the network. The units would then plug into the existing network. The key to having a successful network would be to make sure that the right pieces are brought into the theater and that all of the systems that are brought in are interoperable. Making sure that the right equipment is brought to the theater would be a logistics but not an interoperability problem. Staging components in theater would help in assuring the right set of parts for connectivity. The MSE would be brought in by the Army, and the Marine Corps would bring in their Tactical Data Network (TDN) which should be fielded by the next century. Other units could bring in mobile cellular systems that could be used for wireless LANs. Ships could connect to the network through the radio portion of the network. Host nation links could be used for connectivity to the United States. Also, GBS systems could be used for connectivity with the US.

B. DESIGN ISSUES

The design of this network has to be such that components brought in by units can be easily connected to other units without degradation of the network. The network has to be scalable to meet the needs of everyone on the battlefield. The network can start out as radio-based, but as more non-mobile command, intelligence, and logistic centers enter the battlefield environment a terrestrial WAN should be added to handle traffic and relieve some of the congestion on the radio WAN.

A flexible backbone is needed to make the network scalable. This can be achieved by designing each sub-net with the capability of plugging into each other.

This can be achieved by using routers that can pass the data from one sub-net to the other. A terrestrial backbone could be easily integrated into the network as the need arises. This integration is important for making this network flexible.

An end system should have compatibility with the Open Systems Interconnection Reference Model (OSI) top four layers. The top four layers in this model are application, presentation, session, and transport layers [Ref. 12]. In order for end systems to be good network citizens they must be able to handle the top four layers. The application layer is where conversion of terminal input or output from an application program is put into a message block. The presentation layer is where format definition, encryption, and compression of the data takes place. The message block beginning and ending marks occur in the session layer. The session layer also determines if half or full duplex transmission will be used. The transport layer divides very long message blocks into shorter blocks for transmission, adds a sequence number to each block, adds a checksum for error detection, checks for duplicate blocks, adds security to message blocks, and services for missed chunks.

Similar applications in all systems have to be compatible. The application layer would have to accept common data formats such as email, imagery, and data from tactical data links. There would be a need to conform to interoperable applications that would be used over the network. For instance, e-mail user agents must handle body parts the same way, or else the files sent over the

network would be useless to the receiver. This does not say that everyone has to use the same programs but that the programs used have to meet the standards.

The network layer chunks the message down into predetermined-size packets, attaches the addresses and sequence numbers to the packets, identifies the routes for the packets through the network and then passes the packets to the data link layer. Of course, the use of IP (Internet Protocol) is key to success of the network. The use of IP in the network layer makes for a smoother transition in the data link and physical layers which are beneath the network layer. IP should be used in the routers and other internetworking hardware. IP would have to be established in the current sub-nets before they could be integrated into the network.

The sub-nets not only have to interface with the network layer but they also have to conform with the OSI's data link and physical layers. The data link layer inserts the packet into a frame that becomes the envelope for carrying the packet during transmission. It then adds a frame sequence number and confirms checksums for error detection. A copy of the frame is kept for retransmission in case of a transmission error. It then passes the frame to the physical layer. The physical layer is where the frame is sent out to its destination in the form of a serial stream of bits. The current sub-nets, such as Link-16, Link-11, and Link-4A perform well in the data link and physical layers but they do not interface well with the network layer.

With these OSI layers ingrained in networks that will comprise the battlefield network, the connection of these networks will be simplified thus making them, as is referred to in the commercial world, plug and play. If current systems cannot be adapted to conform to IP and the OSI model then they should be replaced by systems that meet this requirement. Current networking COTS and GOTS equipment meet these requirements.

Other end systems such as radars should have network compatible LAN, logical, and management interfaces built into them. This would ensure that information produced by these end systems could pass over the network to other end units that need this data. This would allow end units to coordinate attacks on enemy forces. An example of this would be that a Patriot battery could see the radar returns from an Aegis cruiser and vice-versa. This would help in getting better shots at incoming missiles for either platform.

High availability requirements need to be built into this network. High availability has three main principles. They are elimination of single points of failure, provision of reliable crossovers, and prompt detection of failures [Ref. 13]. Figure 11 represents two local area networks connected to a wide area network via routers. If either router suffered a failure it would be cut off from the network until repairs are accomplished. The information that this LAN produces or consumes could be life-critical. To ensure that the data gets through the WAN or from the WAN to the LAN, the single point of failure should be eliminated.

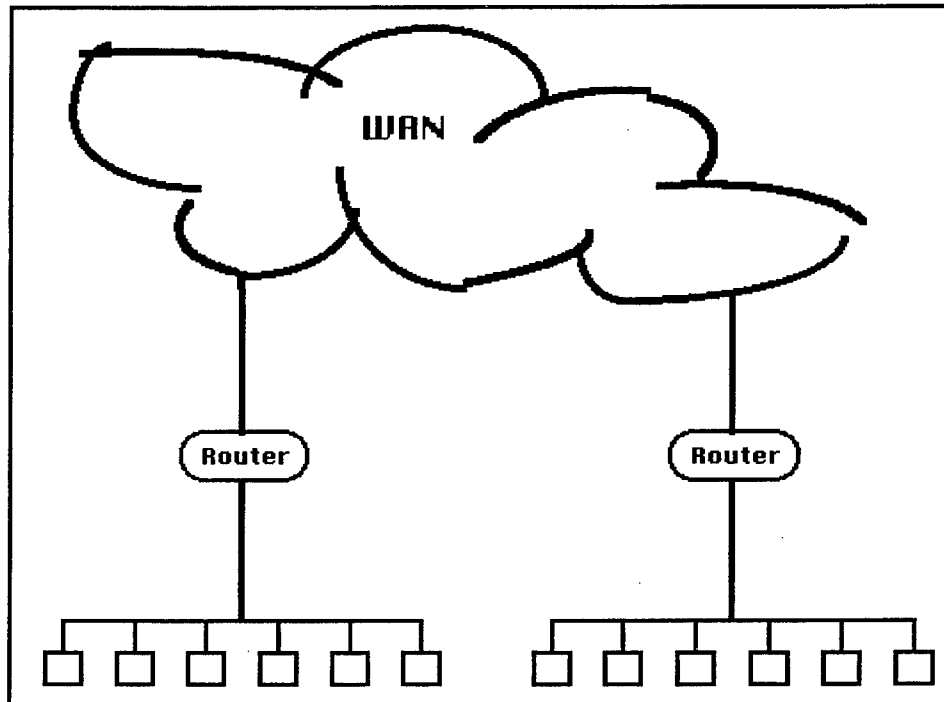


Figure 11 Single Points of Failure After Ref. [13]

Figure 12 shows one way to eliminate this point of failure. Notice that not only are the routers interconnected but also the LANs are interconnected. The dual interconnections are the ideal case but may not be practical. For the sub-nets to be interconnected they must be homogeneous. These interconnections provide the reliable cross connections. This would help eliminate single points of failure. With this setup in Figure 12, data could bypass trouble spots and reach its destination. Now this approach needs to be incorporated into the building of the network. During every phase of development, all aspects of the layout should be looked at for single points of failure.

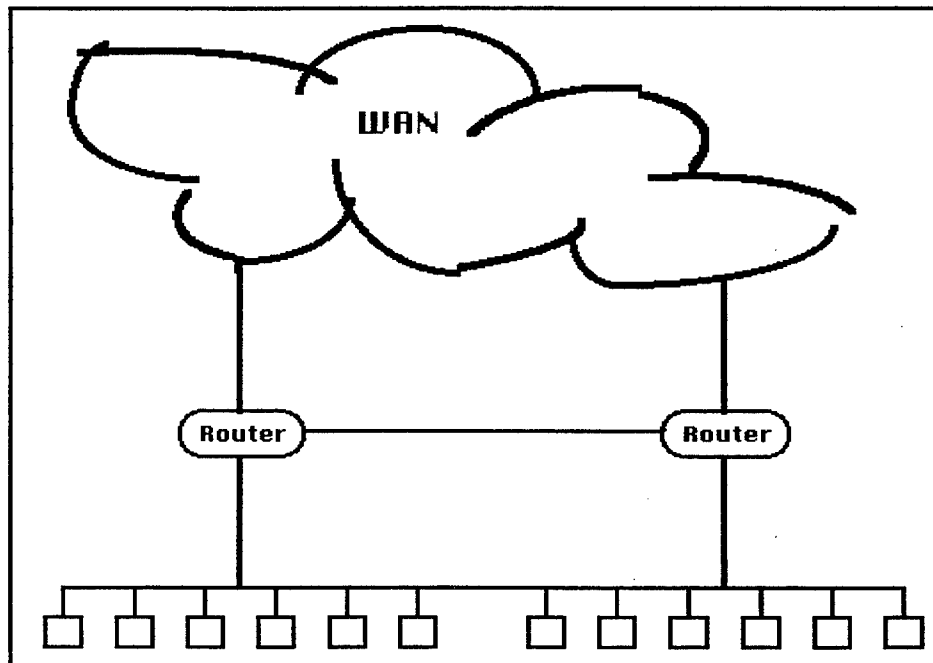


Figure 12 Eliminating Single Points of Failure After Ref. [13]

The detection of failures falls under network management and the network management system (NMS). A NMS will have to be user friendly and easy to learn. It should be graphically oriented, but also have the capability for command line interface to meet all networks managers' requirements. The NMS should have good functional capability in the OSI management framework's five functional areas. These areas are fault management, performance management, configuration management, accounting management, and security management.

A NMS with liberal use of hypermedia would help the network managers quickly isolate trouble spots in the network. Hypermedia could be used by the network managers to view the topology of the network at any level. With a graphical user interface, a network manager could select a portion of the network.

Once the portion was selected the next layer of the topology would appear. This would be very useful in helping to isolate trouble spots on the network. If a trouble spot was located, the color of the device on the topology would change based on the severity of the degradation in the device. A network manager could then click on the device and the inventory management database would provide information on the type of device it is and what other devices it is connected to. This would expedite getting repairs accomplished and minimize down time in that area. As the network grows, the NMS should be adaptable to easily integrate new LANs and other components.

For the non-radio-based LANs, a Fiber Data Distributed Interface (FDDI) ring with optical fiber connectivity is recommended by the author. FDDI uses two counter-rotating rings. Each node connected to the rings can detect failures. With the dual-attachment station (DAS) which physically connects to both rings, a failure of a node will not bring down a network. The DAS uses the undamaged ring to reroute the data thus isolating the failed node and keeping the network functioning [Ref. 12]. Figure 13 is a pictorial representation of isolation of a failed node. With connections on a fiber FDDI ring, optical bypass switches should be installed to allow data to pass around downed nodes. Downed nodes could be either failed, turned off, or in the process of being repaired. The FDDI ring could be easily attached to other network components. Fiber optic cable would also provide a high speed link for the network.

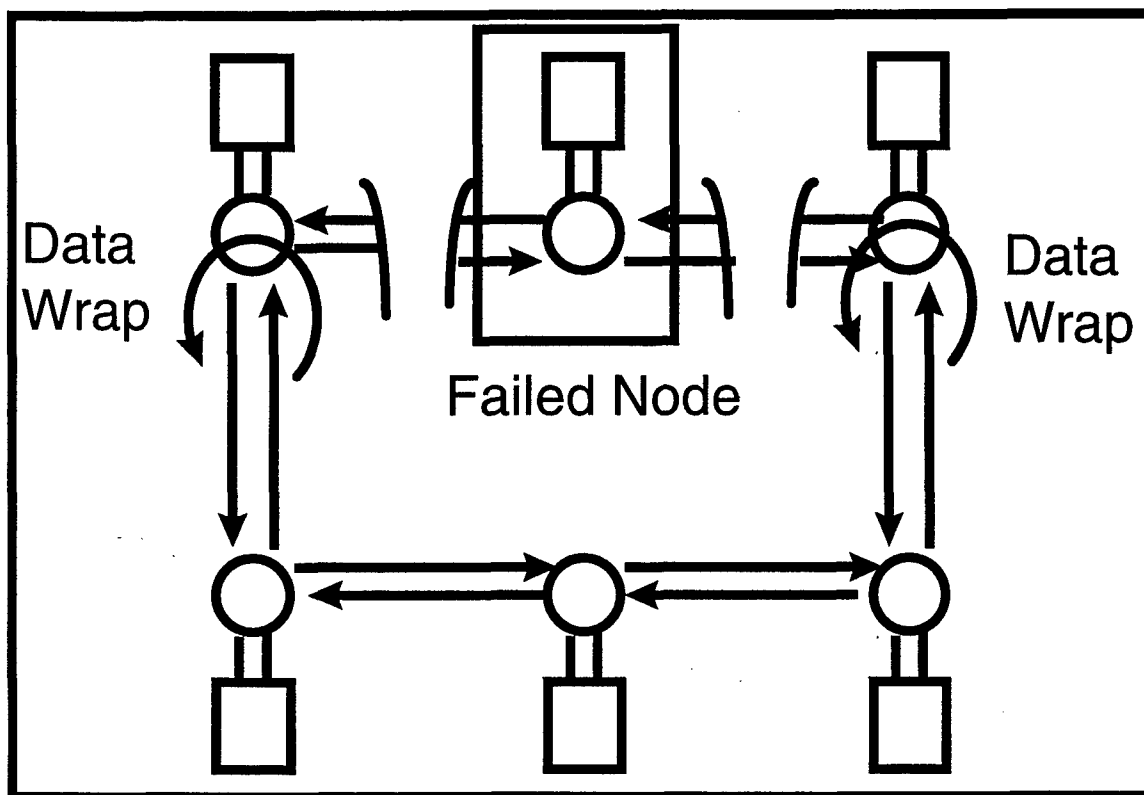


Figure 13 FDDI Isolating a Failed Node From Ref. [13]

If the design factors are taken into account with each new acquisition and if upgrades are made to existing networks, the battlefield network can be achieved by DOD and provide lasting connectivity for the battlefield. The time has come for more networking solutions to support the way that the armed forces conduct business in the battlefields or peacekeeping missions of tomorrow.

V. CLOSE AIR SUPPORT SCENARIO

A. BACKGROUND

This scenario will involve three aircraft, two Navy F/A-18s and a Marine Corps AV-8B. The AV-8B has primary tasking for close air support (CAS). The AV-8B's base of operations is a land base while the F/A-18s are carrier-based. The F/A-18s have primary tasking of a bombing mission but have alternate tasking of CAS if needed. The network battlefield as described earlier is in place. All aircraft are equipped with the capabilities to access sub-nets and have UHF/VHF, HF and cellular radios. This scenario will focus on information passing and the switching of networks.

B. PREFLIGHT

During preflight the F/A-18s are connected by cable to the aircraft carrier's LAN. The AV-8B during preflight operations connects to the airbase's LAN. The mission computer loads the latest update on target information. Friendly position information is also uploaded. The carrier's and airfield's databases are updated by the ordnance personnel who put the weapons on the aircraft. If there is any problem with any of the aircraft's systems the parameters could be downloaded to the maintenance personnel of the aircraft's squadron.

C. FLIGHT MISSION

The AV-8B launches and proceeds on station. The pilot on his way to the target area switches to the LAN of the company that he is going to support. The reason for the switching to a different LAN is not an issue of receiving information

but is a matter of physical location. The LAN of the company happens to be in the physical area of the AV-8B. By connecting to the company's LAN, information could be passed quicker between the pilot and the company. A message is sent to the forward air controller (FAC) in that area that contains the aircraft's weapon load, status, and position information. This could be automatically sent or manually sent by the pilot depending upon how the aircraft's software is set up to handle messaging. The message travels through the company's LAN through the network to the FAC's LAN. Friendly position information is updated as well as target information. This information is displayed graphically on the pilot's display panel. The pilot's display is automatically updated at a predetermined interval. The updates occur because the company's LAN is sending constant updates to the pilot. Position information on this LAN is sent out automatically by all units to all units connected to the LAN. The updates are handled by the aircraft's computer. If voice communication is needed the pilot can use any of the radios for that purpose. After completing the mission the aircraft returns to the airfield. On the way back to the airfield, the pilot can send mission information through the network to the FAC or anyone else who needs the information. If the pilot has enough fuel and ammunition the FAC could decide to use him in another sector for CAS. He can also send information concerning the aircraft back to his unit. This will help in turnaround time and maintenance repairs.

The F/A-18s in route to their bombing mission get continuous updates of the friendly and known enemy forces near their target through the FAC's LAN. The

continuous updates are simply a matter of the FAC forwarding this information to all aircraft in their area of control. They could have received this information from anywhere in the battlefield. In fact, during preflight they received this information by accessing the FAC's database through the carrier's LAN which is connected to the battlefield network via routers. Their target is an enemy power plant. They notice (by an icon on their tactical display) that a reconnaissance platoon is near their target. The flight lead selects the icon and the platoon's information is displayed. The flight lead notes the platoon leader's address and sends a message through the network asking if the platoon has a laser designator. This message could be sent manually or through the selection of the address on the display. The graphical user interface on the displays are user friendly. This would be like selecting an icon on a computer. The platoon leader sends a message back stating that they have one. The platoon leader is equipped with a handheld device that has the capability of displaying a tactical map with an overlay of the tactical picture that is constantly updating. The tactical map is on a CD-ROM which is housed in the device. The device is connected to the network via a wireless LAN. The device has software capable of sending and receiving messages and other types of data. The device also has the capability of connecting to a digital camera for sending imagery taken on the battlefield. The flight lead sends another message asking if they would use it to guide their bombs into the target because this would increase the standoff distance of the aircraft.

After the aircraft drop their bombs, they send the footage shot by the camera on the aircraft back to the area's command and control (C2) node for battle damage assessment. The capability of sending the imagery and other sensor information from the aircraft is available because the aircraft's database stores this information. Through the aircraft's computer the pilot can select this information and send it to anyone connected to the network. The reason that the information is sent to the C2 node is doctrinal in nature and not a limitation of the battlefield network. The platoon also sends pictures of the bombed power plant back to the C2 node. The C2 node will make a decision if another attack is necessary. This decision is based on the BDA and the reports from the pilots and the platoon leader. If another attack is warranted the C2 node will determine what assets are at its disposal and check the weapon load reported by the units and redirect them as needed. The C2 node will make this determination based upon the Air Tasking Order (ATO) and by checking with the FAC for what assets they could redirect to re-attack the power plant. They would be able to determine what weapons are on the aircraft because all aircraft report their weapon load to the FAC in their area. Another way that the C2 node could determine what assets to use would be to look at the tactical picture of the area and check the ATO to see which aircraft would have the weapons needed to bomb the power plant. The C2 node does not need the F/A-18 for their secondary CAS mission. They are sent back to the carrier.

D. POST MISSION

On the way back to their respective landing sites all aircraft switch from the sub-nets that they were on to their landing sites' LANs. There they download pertinent mission data and upload landing information. They can also send maintenance personnel messages that contain information on aircraft status. This would help maintenance personnel in quickly turning around the aircraft for future missions. The ordnance personnel would know what ordnance was expended. For the aircraft carrier this information would help in knowing where to park the aircraft upon landing. This would help the carrier to organize for the next cycle of flight operations.

E. SUMMARY

Currently, the scenario described in this chapter is handled mostly by voice communications. This scenario had all information passed over the battlefield network. This author does not suggest that voice communication should not be used, but much information could and should be passed over the network. The author does suggest that by having a battlefield network, operations could be better carried out and that interoperability is improved between different services. Positioning information should be passed over a network so that when conducting CAS missions, the pilots' situational awareness is enhanced.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

Communication in the armed forces in the continental United States is turning towards networking. More personnel are communicating with email via the internet. More DOD agencies are putting up web pages on the world-wide internet. As a natural extension to this connectivity in the United States that there will be a natural progression to have a battlefield network. With joint cooperation among the services and the other DOD agencies, the battlefield network could and should come into existence. The approach provided in this thesis is but one of several alternatives. If the recommendations made in this thesis are followed, the battlefield network will provide robust communications that could expand as the need arises.

Each service has its own systems for communication. Some of these systems such as Link-11 and Link-16 are shared by other services. Not everyone in the service have access to the information that is carried over these systems. Interoperability should be a standard for all of the services. The only way to achieve interoperability is for the services to agree that any future systems would have the capability to communicate with other services' systems. The next step would be to change the way that we design and buy systems. It is time for the armed forces, in this time of dwindling budgets, to look to the commercial world for products that can be purchased to supplement military-specific communication systems. What cannot be purchased then can be developed by the armed forces

to fit the needs. However, the systems must be able to be integrated. The functionality described earlier needs to be incorporated.

The battlefield network will eventually be realized. The quality of this network will depend on the design and how the services put it together. Stovepipe systems are costly and cannot be supported properly. The warfighter of the future needs communication abilities that transcend service boundaries. Interoperability among the services will be required at the lowest level of the chain of command as more operations conducted by DOD are joint in nature.

B. RECOMMENDATIONS

The concept of the battlefield network brings up many doctrinal issues. Current communication systems in DOD's inventory support a hierarchical chain of command. A networked battlefield can support a more flattened chain of command. Before the network is implemented the doctrinal issues should be studied. For instance, in this thesis a C2 node was placed in the network for illustration purposes. The C2 node was used for positive control over target selection. The doctrinal issues of how control will be set forth in a battlefield will have to be decided upon. Whether positive control or control by negation is used, the battlefield network can support either form of control. The battlefield network would have impact on the ROE of the future battlefield. Doctrine for the battlefield network should be agreed upon by all of the services. The doctrine will help the forces making up the network function more efficiently and effectively due to all of the service components working on the same level.

Security issues were not discussed in detail in this thesis. Security will play a big role in the success of the battlefield network. Further study in this area is warranted. Some of the issues involved are how to allow allies access to the network, the security of the host nation's infrastructure, and how to protect the network from enemies' attempts to destroy the network.

There should be future studies in how DOD can make current tactical data networks and datalinks fit into the networked battlefield. The integration of these networks and datalinks are key to full interoperability. If these systems cannot be integrated without enormous cost or difficulty then they should be replaced by systems that can be easily integrated into the network.

The program managers for end systems, such as Joint Maritime Command Information System (JMCIS), aircraft, tanks and weapons that need external input, should ensure that their systems comply with the top four layers of the OSI model. This would allow the end systems to easily connect to the network. This should be one of the first considerations in any new program and should also be one of the first upgrades to current systems in inventory.

The program manager (PM) for the Defense Information System Network (DISN) and other network PMs should ensure that their networks comply with IP and the bottom two layers of the OSI model. This would also ensure that compatibility with end systems exist. The PMs for the tactical datalinks should look into the best way of upgrading their links to meet the requirements that were suggested in this thesis.

The PMs for the radars and other sensors data-gathering end systems should make sure that they have LAN, logical, and management capabilities built into them so that they can be brought to the field and be connected to the network. Their data packaging should meet the requirements that were put forth in this thesis. Some of these systems may not be able to be updated without enormous cost. If the cost to upgrade these systems is too much for the budgets then alternatives to these systems should be looked at for future development.

Each of the services should look at their service platforms and review the input and output of these platforms to see if they are interoperable with other services' platforms. An example of interoperability would be that distance measuring devices use the same standards. It would be hard to compare data from different platforms if their output was different. If there are differences then conversion factors would have to be implemented or the adoption of one standard would have to occur.

LIST OF REFERENCES

1. *Microsoft Encarta Multimedia Encyclopedia*, Microsoft Publishing CD/Rom, 1994.
2. *Joint Command, Control, Communications, and Computer Systems Descriptions Volume II*, 1995.
3. MIL-STD-188-203-1A, *Military Standard Interoperability and Performance Standards for Tactical Digital Information Link (TADIL A)*.
4. *Understanding Link-16 A Guidebook for New Users*, U.S. Navy Center for Tactical Systems Interoperability.
5. *Understanding Link-11 A Guidebook for New Users*, U.S. Navy Center for Tactical Systems Interoperability.
6. *Understanding Link-4A A Guidebook for New Users*, U.S. Navy Center for Tactical Systems Interoperability.
7. *Link-16 Communications Planning User's Guide Part III*, Naval Command, Control, and Ocean Surveillance Center, RDT&E Division, Warminster, PA, April, 1994.
8. Hudson, Erwin, C., "Direct Broadcast Technologies Applied to MILSATCOM". American Institute of Aeronautics and Astronautics by TRW Space & Electronics Group, Redondo Beach, CA, 1995.
9. "SINGARS SECOND TO NONE", General Dynamics fact sheet.
10. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, Joint Pub 6-0, Joint Chiefs of Staff, May 1995.
11. *JOINT WARFARE OF THE US ARMED FORCES*, Joint Pub 1, Joint Chiefs of Staff, November 1991.
12. Fitzgerald, Jerry, *BUSINESS DATA COMMUNICATIONS Basic Concepts, Security, and Design*, 1993.
13. Buddenberg, Rex, A., IS4502 Telecommunications Networks class notes, <http://dubhe.cc.nps.navy.mil/~budden/lecture.notes/net-centric.html>.

LIST OF DISTRIBUTION

1. Defense Technical Information Center.....2
John J. Kingman Road., Ste 0944
Ft. Belvoir, VA 22060-6218
2. Dudley Knox Library2
Naval Postgraduate School
411 Dyer Rd.
Monterey, CA 93943-5101
3. Chairman, Code CC1
Naval Postgraduate School
Monterey, CA 93943-5101
4. LT. Christopher B. Henderson.....2
P.O. Box 1142
Highland City, FL 33846